**EXPERIMENT 10**

**NAME:** Khan Mohd Aaquib Sameer **ROLL NO:** 22CO21

**SUBJECT:** Computer Network (CN) **YEAR:** TECO

**Aim :-**

Implementation of Network discovery using discovery tool (Nmap)

**Theory :-**

Network discovery using discovery tool (Nmap).Nmap, also known as network mapper,

is a free and open-source security tool widely known for its powerful network discovery, enumeration and security auditing abilities.

Network administrators utilize Nmap to establish a network map and get more

information about what’s going on inside the network: which hosts are online,

what ports are open, which services are offered, and more.

The quickest way to get up and running is by installing Nmap through the APT package manager:

**sudo apt install nmap**

Nmap optimizes port scan speed by first checking if the target is online before

attempting to scan any ports. This is called host discovery or ping scanning and is

enabled in every scan by default.

*aiktc@CO-LAB1-12:~$ nmap 172.16.101.12*

*Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-25 12:47 IST*

*Nmap scan report for CO-LAB1-12 (172.16.101.12)*

*Host is up (0.00011s latency).*

*Not shown: 996 closed ports*

*PORT STATE SERVICE*

*21/tcp open ftp*

*22/tcp open ssh*

*80/tcp open http*

*8080/tcp open http-proxy*

*Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds*

*aiktc@CO-LAB1-12:~$ nmap -sn 172.16.101.12*

*Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-25 12:52 IST*

*Nmap scan report for CO-LAB1-12 (172.16.101.12)*

*Host is up (0.00024s latency).*

*Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds*

Running a host-discovery-only scan is possible in case we only want to see which hosts are online:

*aiktc@CO-LAB1-12:~$ nmap -sn 172.16.101.2-13*

*Starting Nmap 7.80 ( https://nmap.org ) at 2024-09-25 13:13 IST*

*Nmap scan report for 172.16.101.3*

*Host is up (0.00045s latency).*

*Nmap scan report for 172.16.101.8*

*Host is up (0.00044s latency).*

*Nmap scan report for CO-LAB1-12 (172.16.101.12)*

*Host is up (0.000041s latency).*

*Nmap done: 12 IP addresses (3 hosts up) scanned in 1.41 seconds*

**Conclusion :-**

Nmap is an efficient tool for network discovery and security auditing. By performing port and host discovery scans, Nmap helps identify active hosts, open ports, and running services within a network, providing valuable insights for network management and security.